



## Ejercicio Práctico 2

 **Tema:** Validación de Entradas y Prevención de Ataques SQLi/XSS

---

### **Objetivo del ejercicio:**

Aprender a identificar entradas inseguras en un formulario web y aplicar una solución básica para prevenir vulnerabilidades como SQL Injection y XSS.

---


### **Instrucciones:**

1. Observa el siguiente fragmento de código PHP, utilizado para buscar un usuario en una base de datos:

```
<?php
$usuario = $_GET['usuario'];
$query = "SELECT * FROM usuarios WHERE nombre = '$usuario'";
$resultado = mysqli_query($conexion, $query);
?>
```

### 2. Preguntas:

a. ¿Qué vulnerabilidad presenta este código?

- Ninguna
- XSS
- Inyección SQL 

---

b. ¿Qué entrada podría utilizar un atacante para explotar esta vulnerabilidad?

- juan
  - ' OR '1'='1' ✓
  - admin123
- 

c. Reescribe el código usando una consulta preparada (*prepared statement*) con `mysqli` para mitigar el riesgo.

---

### Solución esperada:

```
<?php
$usuario = $_GET['usuario'];
$stmt = $conexion->prepare("SELECT * FROM usuarios WHERE nombre = ?");
$stmt->bind_param("s", $usuario);
$stmt->execute();
$resultado = $stmt->get_result();
?>
```

---

### Reflexión final:

¿Por qué es importante validar y sanitizar las entradas del usuario incluso cuando se usan consultas preparadas?

---